快充设备或存安全隐患 被攻击后可能烧毁手机

“充电5分钟通话两小时”……随着智能充电设备的普及，各大厂商都在不断革新自家产品的快充技术。一直以来，围绕快充的安全性存在着不少疑虑，其中包括对智能设备和电池的影响，以及充电技术本身是否存在安全隐患。

近期，腾讯安全玄武实验室发布了一项研究报告，其中主要提到了一种被命名为“BadPower”的安全问题。报告指出，研究人员通过对市面上35款采用了快充技术的充电器、充电宝等产品进行了测试，发现其中18款存在安全问题。攻击者(黑客)可通过改写快充设备固件中的程序代码来控制充电行为，可造成被充电设备元器件烧毁甚至爆炸等严重后果。

那么，什么样的快充设备易受到“BadPower”威胁？物理世界与数字世界的边界开始模糊，新型安全威胁不断出现，需要怎样来应对？就此，记者采访了有关专家。

A 攻击包括物理接触与非物理接触两种

相比传统充电器，快充设备更加智能，其芯片内部的固件上运行着一套程序代码，相当于快充设备的“大脑”，可以控制并调整快充设备与受电设备之间的充电电压，甚至可以与受电设备交换数据等。

“但是，作为控制和调整充电过程的核心，快充设备上运行的程序代码并没有得到很好的保护。”清华大学网络科学与网络空间研究院副教授张超介绍说，很多快充设备没有设置安全校验，通过受电设备就能毫无阻碍地接触到其程序代码，并能够实现对程序代码的替换；另外，还有部分快充设备的程序代码并不完善，其存在的安全漏洞很容易被攻击者所利用，进而引导其去执行错误或者恶意的行为。

在本次腾讯安全玄武实验室发布的“BadPower”问题报告中，攻击者是如何实现改写固件中的程序代码的？

记者了解到，“BadPower”的攻击方式包括物理接触和非物理接触。报告指出，攻击者发动物理接触攻击，主要是通过直接更换充电宝、快充转接器等设备固件，或利用手机、笔记本电脑等连接快充设备的数字终端改写快充设备固件中的代码，从而实现对充电过程中的电压电流等加以控制。

“具体来说，攻击者通过入侵充电设备改变充电功率，致使受电设备的元器件被击穿、烧毁，还可能给受电设备所在物理环境带来安全隐患。”福州大学数学与计算机科学学院院长助理、网络系统信息安全福建省高校重点实验室主任刘西蒙教授介绍说。

据了解，腾讯安全玄武实验室发现的18款存在“BadPower”问题的设备里，有11款设备可以进行无物理接触的攻击。

“当攻击者无法直接物理接触快充设备时，可以通过网络远程把攻击代码植入受电设备，当受电设备与快充设备连接时，攻击代码就可以直接替换掉快充设备固件上的程序代码。”张超说。

当攻击者替换了快充设备固件的程序代码后，一旦有新的受电设备连接到该快充设备，就会面临电压攻击的威胁。

B USB接口可能成为风险入口

据了解，这18款存在“BadPower”问题的设备，涉及8个品牌、9个不同型号的快充芯片。

“只要充电器同时满足不允许修改固件中的代码、对固件进行安全校验两个条件，就不会出现类似安全风险。”刘西蒙指出，不同快充协议本身没有安全性高低的差别，风险主要取决于是否允许通过USB口改写固件中的代码，以及是否对改写操作进行了安全校验等。

腾讯安全玄武实验室针对市面上的快充芯片进行了调研，发现近六成可通过USB口更新代码，安全风险不容忽视。那么，“BadPower”是否对用户隐私安全问题构成威胁？

“市场上的正常快充设备的体积和硬件能力受限，无法执行复杂的恶意行为，因此，当前披露的‘BadPower’攻击并不会造成用户隐私泄露问题。”张超说。

但是，如果厂商为快充设备提供了较强的计算能力，或者攻击者将伪造的快充设备送到用户手中。那么，攻击者就有机会利用快充设备发起更复杂的攻击，可能会给用户带来严重的安全风险，如隐私数据泄露、智能设备被控制等。

近年来，类似“BadPower”的攻击事件也层出不穷。腾讯安全玄武实验室此前还曾披露过一种“BadBarcode”攻击，即通过恶意的条形码可攻击扫描仪，进而控制连接扫描仪的设备（如收银电脑）；还有的是通过对U盘的固件进行逆向重新编程，执行恶意操作；另外还曾出现利用二维码入侵智能设备进行攻击、利用充电桩攻击电动车等安全事件。

C 安全隐患问题需要制造商来根治

针对“BadPower”带来的问题，应该如何有效规避和解决？

“建议用户应该提高安全意识，比如不要给数码产品外接来路不明的设备，包括免费的充电器、U盘等。同时不要轻易把自己的充电器、充电宝等借给别人用。”张超说。

刘西蒙表示，消费者的财产安全权既包括使用商品和接受服务时的人身安全，也包括商品和服务对于消费者其他财产不存在安全威胁。所以，如果用户使用了质量不过关的快充设备导致出现安全问题，可以通过法律程序来保护自身权益。

但是，“BadPower”问题最终还需要制造商来根治。

在技术层面上，充电设备的固件普遍使用单片机来编写程序与调试，不少厂家直接将充电USB接口和调试接口合二为一，这样就会导致设备容易产生安全漏洞、遭受病毒入侵。因此，刘西蒙建议，在技术上应当做到充电USB接口和调试接口分离，并在USB接口和调试接口上同时加密以防止外部入侵。

同时，厂商在设计和制造快充产品时，可通过提升固件更新的安全校验机制、对设备固件代码进行严格安全检查、查补常见软件安全漏洞等措施来防止遭受“BadPower”攻击威胁。

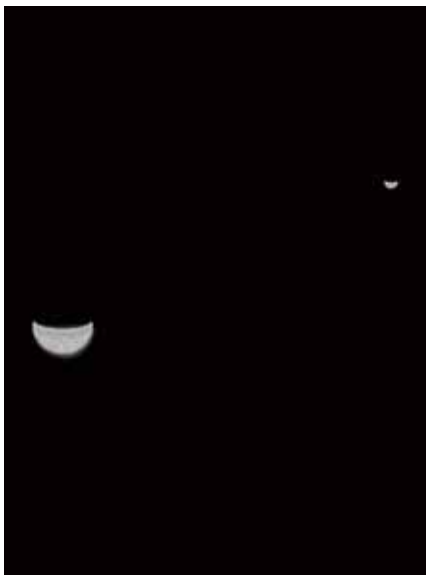
据了解，此前腾讯安全玄武实验室已将“BadPower”问题上报给国家信息安全漏洞共享平台，并和相关厂商沟通，共同推动全行业采取积极措施消灭“BadPower”问题。同时，有业内专家建议，将安全校验的技术要求纳入快速充电技术国家标准。

“BadPower”攻击也再次提醒我们，随着人类生产、生活的数字化，数字世界和物理世界之间的界限正变得越来越模糊。

“其中安全威胁问题的根源，一方面是行业还没有意识到安全前置的重要性，没有把安全做到设计环节；另一方面是对供应链引入的安全风险还没有充分的认识，因此数字安全问题就会变成物理安全问题。”刘西蒙指出，必须加强对数据隐私等方面的安全保护意识。

张超认为，由于技术和成本局限、人为因素等，安全威胁无法完全消除，攻防博弈会始终迭代演进。用户自身提高安全意识是最经济的应对手段，而大力发展网络安全行业，打通产学研生态，依靠专业安全人才和产品提高厂商和用户的防护能力，才是对抗层出不穷的安全威胁的最有效手段。 据新华网

地月合影是怎么拍出来的？



一张由中国火星探测器“天问一号”在奔火途中回眸拍摄的地月合影火了。北京航天飞行控制中心飞控团队与中国航天科技集团试验队密切配合，控制“天问一号”探测器在飞离地球约120万公里处回望地球，利用光学导航敏感器对地球、月球成像，获取了地月合影，国家航天局对外正式发布了这一影像。

这么远的距离、这么快的速度，地月合影的拍摄难度可想而知。29日，记者采访了中国航天科技集团的试验队员，揭秘地月合影背后的故事。

在这幅黑白合影图像中，地球与月球一大一小，均呈新月状，在茫茫宇宙中交相辉映，引发人们对于太空和宇宙的无限遐想，不少网友纷纷在网上留言抒发感受。

据悉，由中国航天科技集团八院控制所研制的光学导航敏感器安装在探测器上，可以在飞近火星的过程中通过对火星成像，利用火星图像计算火星的形心位置和视半径大小，结合估计算法获取探测器相对于火星的实时位置和速度信息。

探测器在太空中，就像轮船航行在茫茫大海上，不同的是飞离地球后没有北斗导航也没有GPS。在基于地面无线电导航实现精确定位的基础上，八院研制团队还给探测器配备了光学导航敏感器，对深空探测相关光学导航方法进行工程验证。

专家指出，与传统的无线电导航不同，光学自主导航可以通过图像目标识别和特征提取，完成位置、速度等导航信息的获取。这也是支撑我国未来进一步走向宇宙更远空间的重要技术之一。此次地月成像即由光学导航敏感器自主曝光拍摄完成。

“光学导航敏感器就好比探测器的‘眼睛’。”八院控制所光学导航专家打了个比方：“有了这双明亮的‘眼睛’，探测器也就有了自主能力，可以自己看着飞向目的地了。”

探测器在飞近火星的过程，八院研制团队将装有长焦镜头的导航敏感器当作一只“千里眼”，最远可以在1000万公里的距离识别火星，还能自主适应火星从点目标到面目标、从弱目标到强目标的火星图像提取，从而实现即使没有外部导航信息，也能够在深空飞行中自主找到前进的道路。

有了明亮的“眼睛”，“天问一号”就可以看着火星再踩下刹车了，而光学自主导航技术也将为我国后续深空探测任务的开展打下坚实基础。

据新华社